Autonomy Assurance for Space Missions

Martin S. Feather (Martin.S.Feather@jpl.nasa.gov)
Jet Propulsion Laboratory, California Institute of Technology

Jet Propulsion Laboratory
California Institute of Technology

Acknowledgements

Contents

- An Information Request!

- What *is* Autonomy?

- *Why* Autonomy for Space Missions?

- *Examples* of Autonomy for Space Missions

- Why *NOT* Autonomy for Space Missions?

- Autonomy Assurance *Challenges* (1 – 5)
  … & Some *Approaches* to Addressing Them

- Recent Related Activities

- Some Current Space Autonomy Assurance Research
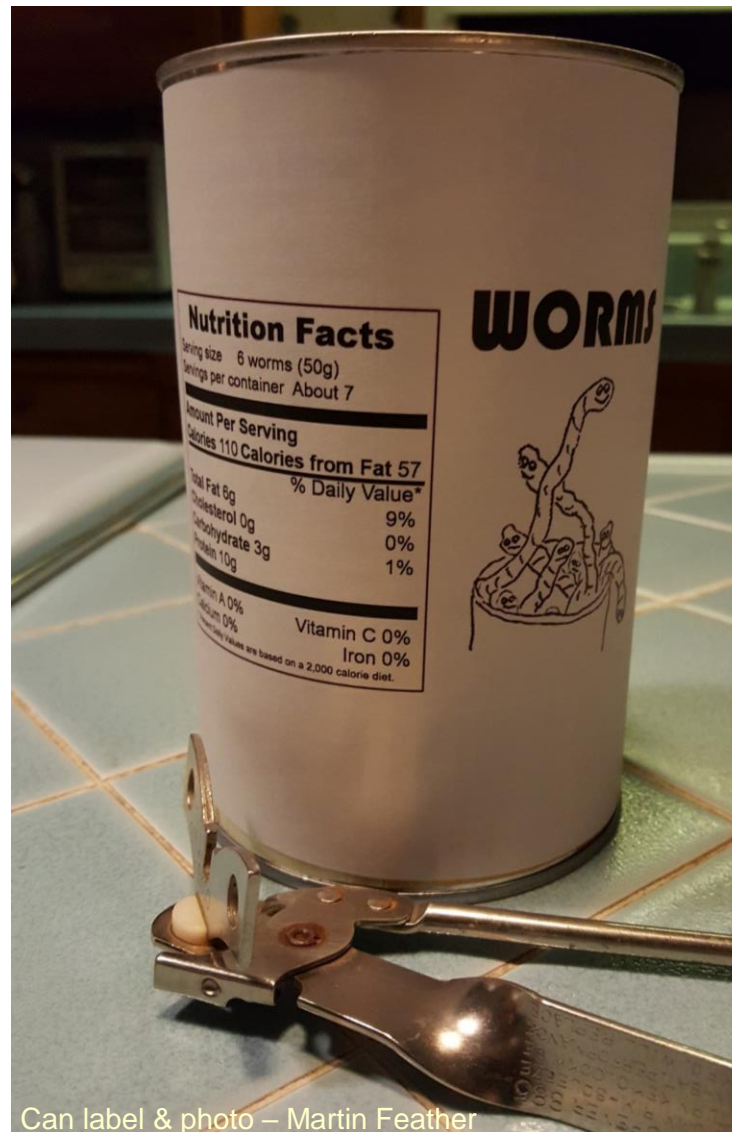
An Information Request!

If you know of:

work on autonomy for space missions,

particularly:

work on *assurance* of such autonomy,

and especially people:

who would be interested in participating in a working meeting to discuss autonomy assurance for space missions,

please let me know!

Martin.S.Feather@jpl.nasa.gov

What *is* Autonomy?

Can label & photo – Martin Feather

What *is* Autonomy?

Autonomy is the capacity of a system to achieve goals while operating independently from external control.

Autonomy is enabled by automation, which is the automatically-controlled operation of an apparatus, process, or system using a pre-planned set of instructions (e.g., a command sequence). Autonomy is also facilitated by artificial intelligence techniques, which enable systems to reason and act in a rational manner to achieve specified goals.

NASA Technology Roadmaps – Introduction, Crosscutting Technologies, and Index
https://www.nasa.gov/sites/default/files/atoms/files/2015_nasa_technology_roadmaps_ta_0_introduction_crosscutting_index_final_0.pdf

What *is* Autonomy?

"I think, therefore I am autonomous"
[René Descartes, extrapolated]

| Perceive | → | Decide | → | Act |
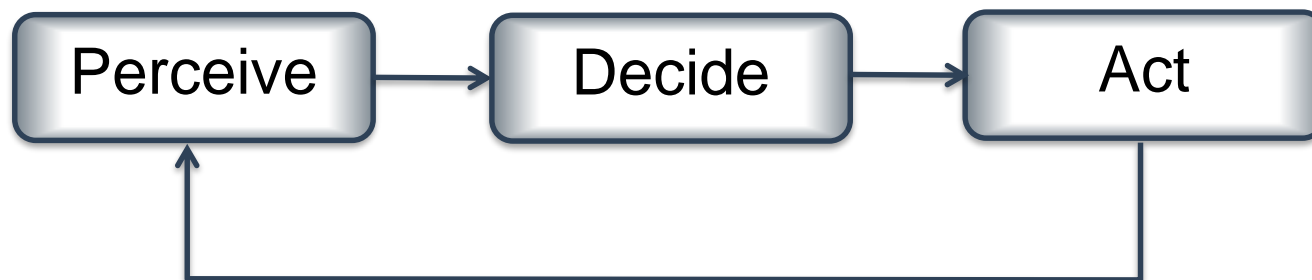
Autonomy [for space missions]: *To make decisions and take actions, in the presence of uncertainty, to execute the mission and respond to internal and external changes without human intervention.*
[Lorraine Fesq & Issa Nesnas, JPL]

Why [Autonomy] for Space Missions?

- Enabling (can't do without)
  - Makes mission possible (achieve ≥ X amount of science with ≤ Y budget…)
    - *E.g., through responses sooner than round-trip light time would permit ground to direct*
    - *E.g., operation of a swarm of 100 spacecraft with << 100 x ground control*
  - Reduces a significant mission risk *providing another layer of protection*

- Enhancing (nice to have)
  - Extra science
    - *E.g., through opportunistic data collection*

Examples of Autonomy for Space Missions

- DS1's **Remote Agent Experiment** (1999)
  https://ti.arc.nasa.gov/tech/asr/groups/planning-and-scheduling/remote-agent/
  - Constraint-based, goal directed planning and execution
  - Livingstone: Mode Identification (model-based diagnosis) and Recovery

- EO-1 https://eo1.gsfc.nasa.gov/ (2000-2017)
  - **Autonomous Sciencecraft Experiment**: "…onboard autonomous decision-making   software … to change a science satellite's priorities without the involvement, or even knowledge, of ground controllers so it can observe unexpected phenomena in its path such as an active volcano"
  - **Livingstone** 2 (L2): "…model-based on-board software that will automatically detect and diagnose failures in satellite's instruments and systems"

- **AEGIS Autonomous Exploration for Gathering Increased Science** (2009-)
  - Mars Exploration Rover Opportunity: "software to analyze images from a wide-angle camera as the basis for autonomously selecting rocks to photograph with a narrower-angle camera"
  - Curiosity Mars Rover: "AEGIS allows the rover to get more science done while Curiosity's human controllers are out of contact"
    https://www.jpl.nasa.gov/news/news.php?feature=6879

Why *NOT* Autonomy for Space Missions?

Risk!

- In-flight risk: impact on mission

- Development risk: schedule & budget

Autonomy Assurance: needed to show that Autonomy Risk is acceptable

Autonomy Assurance Challenges (1)

Autonomy is used for its **ability to respond to a wide range of circumstances** (if there was not a wide range, simple automation would suffice)
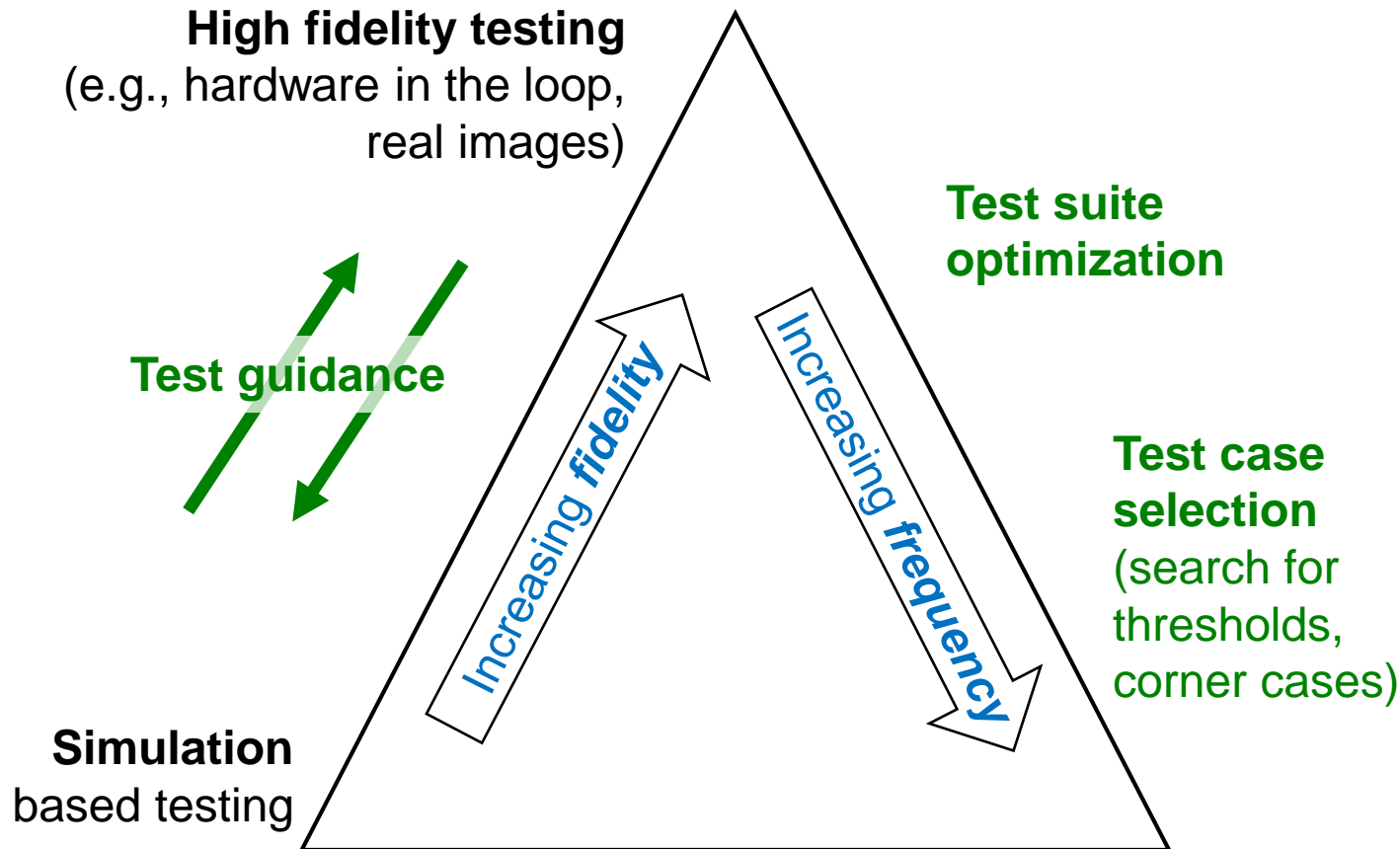
- Too many circumstances to list (e.g., number of possible 512x512 images)

- Infeasible to test all circumstances

- Challenging to accurately mimic those circumstances

- Few opportunities to test/train the autonomy in its system/space context

if P1 then…
elseif P2 …
elseif P3 …
elseif P4 …
elseif P5 …
elseif P6 …
elseif P7 …
elseif P8 …
elseif P9 …
elseif P10 …

…

elseif P262140 …
elseif P262141 …
elseif P262142 …
elseif P262143 …
else …
end if

Addressing Autonomy Assurance Challenge (1)

High fidelity testing
(e.g., hardware in the loop,
real images)

Test suite optimization

Test guidance

Increasing **fidelity**

Increasing **frequency**

Test case selection
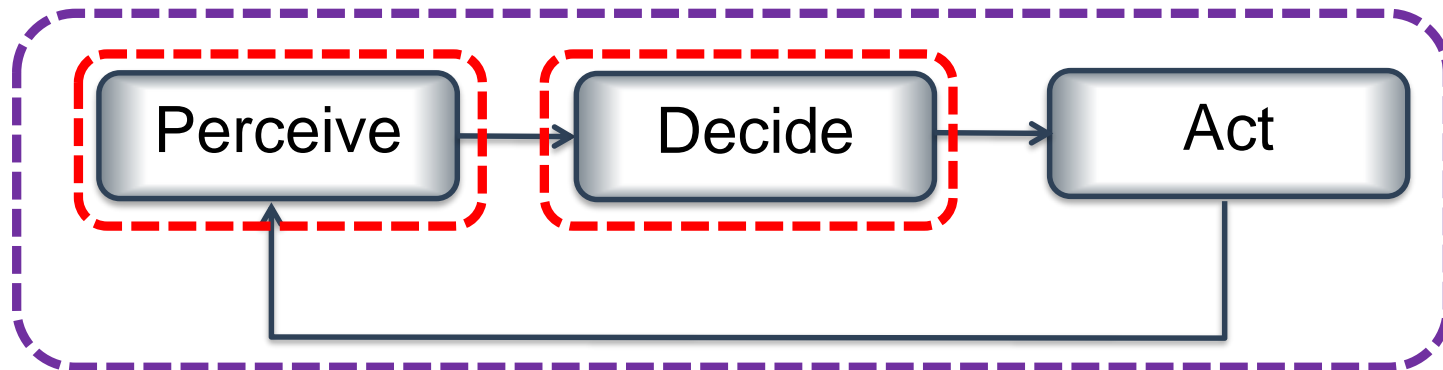(search for thresholds, corner cases)

Simulation
based testing

Speedups/scaleups, e.g.,

"GPU-accelerated Monte-Carlo Simulations" (FY'18 SARP: PI: Spolaor)
"V&V of Complex Autonomy Concepts Using the Cloud" https://techport.nasa.gov/view/90277

Autonomy Assurance Challenges (2)

Autonomy software is atypical and executes *without the opportunity for ground intervention*

- Sophisticated on-board perception algorithms, e.g.:
  – Fault detection
  – Vision processing
- Sophisticated on-board decision algorithms, e.g.:
  – Fault diagnosis
  – Planning and scheduling

Addressing Autonomy Assurance Challenge (2)

Architecture

- **External assessment: "safety monitor" / "runtime verification"**
  - Easier to assure than the autonomy itself

"White box" scrutiny

- **Check the result is right *for the right reasons***
  - E.g., DS1's planner took into account all constraints *

* Feather, M.S. and Smith, B., 2001. Automatic generation of test oracles—from pilot studies to application. Automated Software Engineering, 8(1), pp.31-61.

Autonomy Assurance Challenges (3)

Autonomy software often **model-based**

- The model will be an abstraction (e.g., of hardware)
  - Is it *detailed enough* for the decision needs?
  - Is it *complete* at that level of detail?
  - Is it *correct*?
- Testing:
  - Code coverage *does not imply* model coverage
  - Is the code correct w.r.t. all valid models?
  - Is execution *performance* within bounds (time, memory, bandwidth)
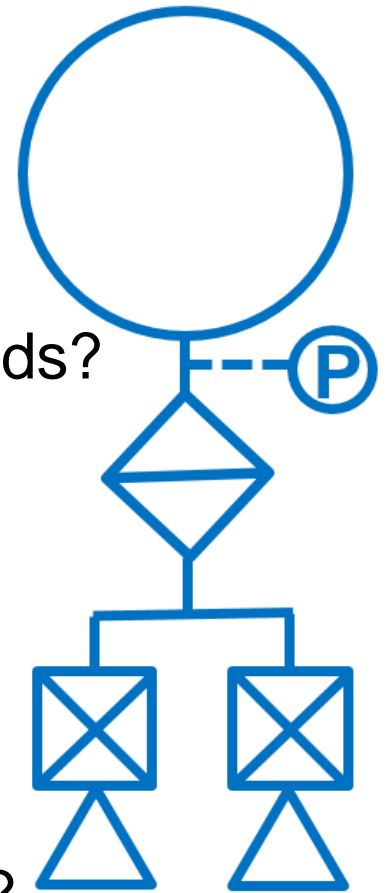
Addressing Autonomy Assurance Challenge (3)

Testing the model

- **Cross-validation with other reasoners, with high fidelity simulations * ***

- **"Parametric Model Analysis" ***

Analyzing the model

- **Formal methods, e.g., model checking ****

* Mahadevan, N., Lowry, M., Schumann, J. and Karsai, G., 2016. DVER: A tool chain for cross-validation and perfection of discrete model-based diagnostic systems. In Aerospace Conference, 2016 IEEE (pp. 1-15). IEEE.

** A. Nikora, P. Srivastava, L. Fesq, S. Chung, & K. Kolcio, "Assurance of Model-Based Fault Diagnosis," 2018 IEEE Aerospace Conference, March 3-10, 2018.

**& Penix, J., Pecheur, C. and Havelund, K., 1998. Using model checking to validate AI planner domain models. In Proceedings of the 23rd Annual Software Engineering Workshop, NASA Goddard.
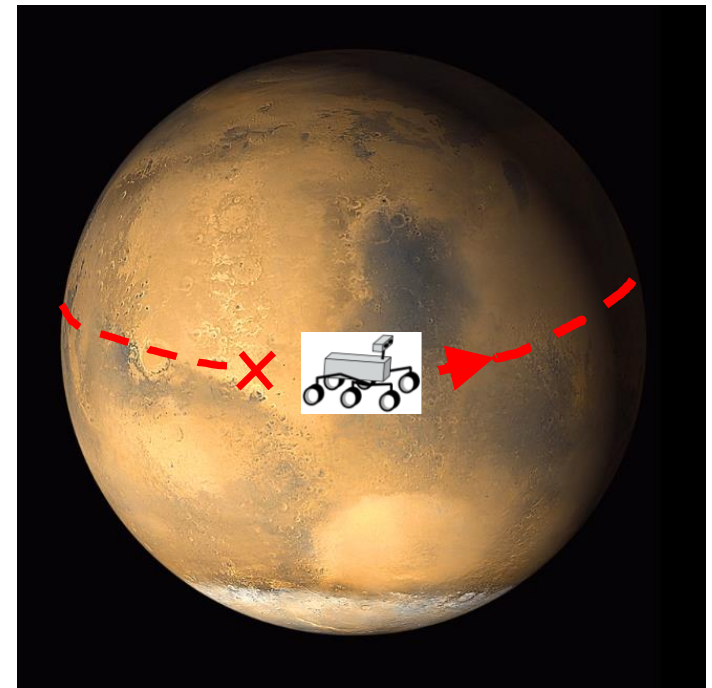
Autonomy Assurance Challenges (4)

Underspecification

Autonomy may satisfy the specification … but in an *unintended* and *undesirable* way

- "Tacit" constraints are hard to elicit…

- and how do you know you have elicited them all?

Drive to that rock 1m behind

(The image of Mars is real, the example is made up)

https://solarsystem.nasa.gov/resources/465/dust-haze-hiding-the-martian-surface-in-2001/?category=planets_mars

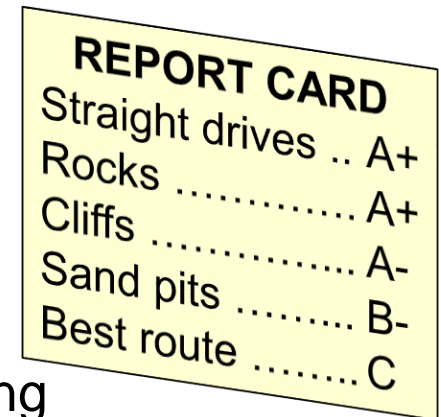# *Addressing* Autonomy Assurance Challenge (4)

Pass/fail from a test oracle is insufficient

- **Visualize/characterize solutions**

Autonomy Assurance Challenges (5)

Perfection may be impossible,
especially for autonomy, e.g.,

- 100% identification of image features
- Optimal planning when time and memory is limited
- Balancing time spent reasoning vs. time spent acting
- Zero false positives and zero false negatives in diagnosis

Assurance needs to:

- Identify conditions under which autonomy is to be trusted
- Identify conditions under which autonomy is not to be trusted (or has not yet been shown to be trustworthy)
- Assure autonomy's recognition of its own (un)trustworthiness and its determination of whether it's better to go ahead, or to stop and call home for help

REPORT CARD
Straight drives .. A+
Rocks .... A+
Cliffs .... A-
Sand pits .... B-
Best route C

Addressing Autonomy Assurance Challenge (5)

Hazard Analysis

- **What might confound autonomy?**

    - E.g., One's own shadow
      is distinctive, but not a feature
      of the ground itself

https://mars.nasa.gov/resources
/5617/
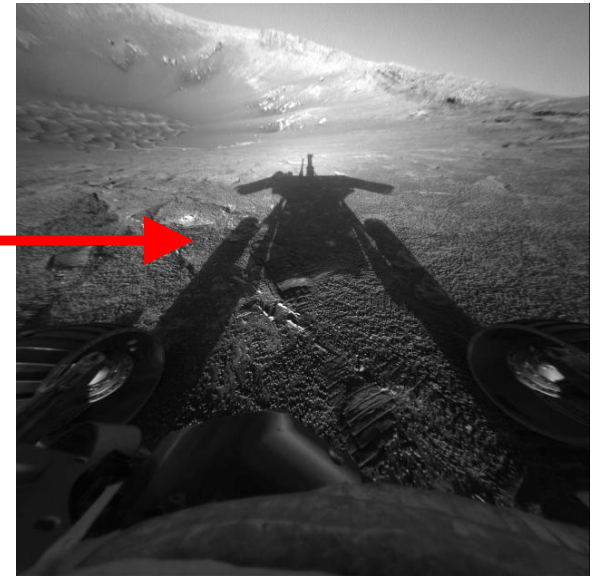
Architecture

- **Internal assessment: "self
  confidence" of autonomy**

    - E.g., DIMES was allowed to *not*
      report a result if it was not highly
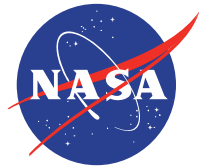   confident of its correctness *

* Yang Cheng; Johnson, A.; Matthies, L. "MER-DIMES: a planetary landing application of
computer vision" Computer Vision and Pattern Recognition, 2005. CVPR 2005.

Recent related activities

- FSW 2017 http://flightsoftware.jhuapl.edu/ (Workshop on Spacecraft Flight Software): **Autonomy Panel** *Adrian Hill - Moderator, Alice Bowman, Dr. Lorraine Fesq, Ronnie Killough, Bruce Savadkin – video at:* https://youtu.be/70QLIYQ0g98

- Workshop on **Assurance for Autonomous Systems for Aviation**, January 2016 https://ntrs.nasa.gov/search.jsp?R=20170000385

- NASA Aeronautics Research Strategic Implementation Plan https://www.nasa.gov/aeroresearch/strategy – Strategic Thrust 6: **Assured Autonomy for Aviation Transformation**

- 2012 Workshop on Engineering **Resilient Space Systems**: Leveraging Novel System Engineering Techniques and Software Architectures http://kiss.caltech.edu/workshops/systems/systems.html

- 2012 Layered Assurance Workshop included "Towards **Safety Assurance of Trusted Autonomy** in Air Force Flight Critical Systems" https://www.acsac.org/2012/workshops/law/pdf/wip.pdf

Some Current Space Autonomy Assurance Research

- Dr. Steve Chien leads an effort to explore the **assurance of an "opportunistic" scheduler**
  W. Chi, S. Chien, J. Agrawal, G. Rabideau, E. Benowitz, D. Gaines, E. Fosse, S. Kuhn, & J. Biehl, "Embedding a scheduler in execution for a planetary rover," to appear in Intl Conf. on Automated Planning and Scheduling (ICAPS) Delft, NL June 2018

- Dr. Seung Chung leads an effort to explore the **assurance of model-based health status determination**
  A. Nikora, P. Srivastava, L. Fesq, S. Chung, & K. Kolcio, "Assurance of Model-Based Fault Diagnosis," 2018 IEEE Aerospace Conference, March 3-10, 2018.

- Dr. Ben Smith leads an effort to explore the assurance of **autonomous rover driving** (e.g., for future Mars rovers)
  B. Smith, M. Feather, & T. Huntsberger, "Hybrid Method of Assurance Cases and Testing for Improved Confidence in Autonomous Space Systems," 2018 American Institute of Aeronautics and Astronautics SciTech Forum's SOF-04, Software Challenges in Aerospace session.

- Dr. Leila Meshkat leads a SARP initiative started in FY18 on "A method to guide **assurance for Autonomous Software and Operations**"
  https://nen.nasa.gov/documents/909012/2611113/FY18+-+Initiative+Summary+-+Assurance+for+Autonomy.pdf/8e7fbb4e-47ed-91af-25e6-9efacef6ec65

- Dr. Mikael Lindvall leads a SARP initiative started in FY18 on "Modeling **Requirements for Autonomy**" https://nen.nasa.gov/documents/909012/2611109/FY18+-+Initiative+Summary+-+Modeling+Requirements+for+Autonomy.pdf/6b804494-bdb2-e25e-cd5c-b7e4651289d3

jpl.nasa.gov